

文章编号: 2095-4980(2018)06-1066-07

用频装备电磁频谱参数泄露机理及防护方法

张余¹, 陈勇¹, 柳永祥¹, 罗明鉴²

(1.国防科技大学 第六十三研究所, 江苏 南京 210007; 2.中国人民解放军 31003 部队, 北京 100029)

摘要: 针对用频装备面临的日益突出的电磁频谱参数安全问题, 分析了电磁频谱参数泄露造成的危害。从电磁频谱参数泄露模式、泄露途径和泄露原因等方面, 研究了电磁频谱参数泄露机理。最后针对重大任务不同阶段的特点, 给出了任务筹划、任务实施和任务结束等阶段的电磁频谱参数泄露防护方法。经过试验进一步验证了其防护方法的有效性, 为开展电磁频谱参数泄露防护工作提供支撑。

关键词: 电磁频谱参数; 电磁频谱参数泄露; 泄露防护

中图分类号: TN911

文献标志码: A

doi: 10.11805/TKYDA201806.1066

Research on the electromagnetic spectrum parameters leaking mechanism and defense approach for the spectrum-dependent equipment

ZHANG Yu¹, CHEN Yong¹, LIU Yongxiang¹, LUO Mingjian²

(1.The 63rd Institute, National University of Defense Technology, Nanjing Jiangsu 210007, China;
2.PLA Troop 31003, Beijing 100029, China)

Abstract: To solve the increasingly prominent problem of the electromagnetic spectrum parameters security of the spectrum equipment. This paper analyzes the harm influence resulted from the electromagnetic spectrum parameters leaking, studies the electromagnetic spectrum parameters leaking mechanism including the electromagnetic spectrum parameters leaking model, approach and reason, proposes the electromagnetic spectrum parameters leaking defense approach in the stage of the task planning, the stage of the task implementing and the stage of the task termination according to the feature of the different stages of task, and its availability is confirmed in the experiment. The research result of this paper will provide support for the electromagnetic spectrum parameters leaking defense.

Keywords: electromagnetic spectrum parameters; electromagnetic spectrum parameters leaking; leaking defense

随着军队信息化程度的提升, 用频装备的角色逐渐从保障装备转变为主战装备, 不但涉及到通信、雷达、导航、制导等领域, 还涉及到电磁攻击、战场感知等, 几乎覆盖了现代战争的所有功能域^[1]。用频装备在正常工作时, 不但要有意向外发射电磁信号, 还可能无意辐射一些无用电磁信号, 这些向外辐射的电磁信号将主要产生三方面的危害^[2-5]: 一是危害周围的人员健康; 二是对周边的电子设备产生电磁干扰; 三是导致电磁频谱参数泄露。前两个方面是各类信息技术设备工作时遇到的普遍问题, 已经有较为成熟的电磁兼容性理论和技术应用于工程实践。但是电磁辐射带来的电磁频谱参数泄露问题却时常被忽视。如果这些向外辐射的电磁频谱参数信息经过空间传播后被第三方高灵敏度的接收设备侦收, 存在被复现和利用的风险, 尤其是在敌对势力在我国周边地区建立起立体化的电磁频谱参数侦收网的大环境下, 用频装备电磁频谱参数面临巨大的安全威胁, 并随着技术的不断发展, 电磁频谱参数泄露给用频装备带来的电磁频谱参数安全隐患日益突出^[6]。如何有效防止用频过程中电磁频谱参数泄露, 确保用频装备安全用频成为目前亟待解决的问题。

1 电磁频谱参数泄露危害

电磁频谱参数泄露实质是用频装备电磁频谱参数信息以电磁信号形式传递到敌方电磁窃收系统, 敌方通过分

析处理截获的电磁信号,从中获取用频装备的地理位置、工作方式、频率特征、使用规律等频谱参数,并加以利用,由此将给用频装备电磁频谱参数安全造成巨大威胁,电磁频谱参数泄露后将可能造成以下主要危害:

1) 暴露实际信息作战能力

信息化作战背景下,大量用频装备在训练和演习中集中使用,将会导致很多电磁频谱参数在不经意中泄露出去,被敌方截获和利用。敌方结合平时搜集的情报信息,根据恢复的众多用频装备的电磁频谱参数信息,可以推断出部队实际信息作战能力。

2) 暴露信息装备能力水平

新研的用频装备需经过大量外场试验检验后才能定型,在此过程中用频装备不可避免地向外发射大量的电磁信号,敌方可借助其侦察能力优势,轻易地窃取用频装备的电磁频谱参数,并基于事先收集的装备技术研究相关的情报资料,推测出装备能力发展现状,甚至可预测未来装备发展趋势。

3) 暴露重要军事阵地分布

重要军事阵地是和平时敌方重点侦察的对象,敌方可利用先进的侦收系统对重要军事阵地中用频装备辐射的电磁信号进行侦收、处理,恢复出电磁频谱参数信息,并通过长期的积累分析推测出重要军事阵地的分布情况,使其成为战时敌方首要打击目标。

4) 暴露兵力部署与作战意图

在未来信息化战争中,用频装备作为主战武器,遍布于整个战场空间,其分布情况跟兵力部署与作战意图紧密相关。如果在用频装备使用过程中,其电磁频谱参数信息被敌方掌握,敌方就可推断出我军兵力部署与作战意图,使其兵力部署与作战意图毫无秘密可言。

电磁频谱参数泄露除了将造成以上危害外,还将产生阻碍国家战略利益拓展、损害国家和军队合理使用电磁频谱资源的权益、阻碍用频装备发展进程等危害。

2 电磁频谱参数泄露机理

2.1 电磁频谱参数泄露模式

电磁频谱参数泄露实际上是从“泄露源”向“窃收系统”有意或无意的信息传输,其过程可比拟为一个完整的无线通信系统,可将其称为“电磁频谱参数泄露等效通信系统”,如图1所示^[2-7],该系统中用频装备是信源,同时也是发射设备,在其工作时除伴随着正常信号发射外,还承载电磁频谱参数信息的发射,用频装备向外发射信息后,在空间电磁噪声干扰情况下,经过无线信道传输到窃收系统中,而窃收系统具有很强的信号接收与处理能力,能够接收提取电磁频谱参数和泄露发射电磁频谱参数。

从电磁频谱参数泄露信息传递角度来看,用频装备电磁频谱参数泄露模式可分为电磁频谱参数泄露直接模式和电磁频谱参数泄露反射模式,其中,电磁频谱参数泄露直接模式指的是用频装备在运行过程中,向空间有意或无意辐射的电磁信号,直接到达敌方电磁窃收系统,被敌方接收处理,并加以充分利用的一种模式。电磁频谱参数泄露反射模式指的是用频装备在运行过程中,电磁信号受地理环境、天线方向性等限制,其向外辐射不能直接到达敌方电磁窃收系统的接收机,而是在空间传播过程中经装备、建筑物等物体反射后,到达敌方电磁窃收系统的接收机而造成的电磁频谱参数泄露的一种模式。

电磁频谱参数泄露必须具备以下条件才能对电磁频谱安全造成危害:一是己方存在主动(有意或无意)向外辐射电磁信号的电磁频谱参数泄露源;二是电磁频谱参数泄露源向外辐射的电磁信号可被敌方接收;三是敌方能够从接收到的电磁信号中提取出电磁频谱参数信息。

2.2 电磁频谱参数泄露途径

电磁频谱参数泄露途径是造成电磁频谱参数泄露,对电磁频谱参数安全造成重大威胁的重要因素之一,可分为辐射泄露和传导泄露^[7-8],如图2所示。辐射泄露主要是用频装备在使用过程中通过天线或用频装备壳体以辐射方式向外泄露,电磁频谱参数泄露信息的电磁能量通过空间传播方式传递或耦合到敌方电磁窃收系统,是电磁频谱参数辐射的主要模式。用频装备在工作时,不仅以用频装备天线正常发射、旁瓣泄露发射和杂散发射等形式有意识地向外辐射电磁波,还可能以等效天线的天线耦合、导线干扰耦合和闭合回路耦合等形式无意向外辐射电

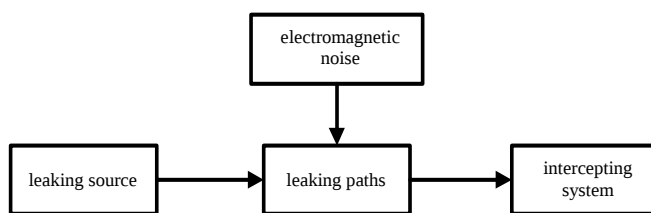


Fig.1 Basic structure of the equivalent communication system of the electromagnetic spectrum parameters leakage

图1 电磁频谱参数泄露等效通信系统的基本结构

磁波。不管是通过用频装备的正常天线,还是等效天线向外辐射的电磁波,通过空间传递后都有可能到达敌方电磁窃收系统,敌方利用其电磁窃收方面的先进技术对其进行窃收、处理,提取用频装备的地理位置、装备型号、方位信息、工作频率、工作带宽、带外杂散、使用规律等电磁频谱参数并加以充分利用,对电磁频谱参数安全形成较大威胁。

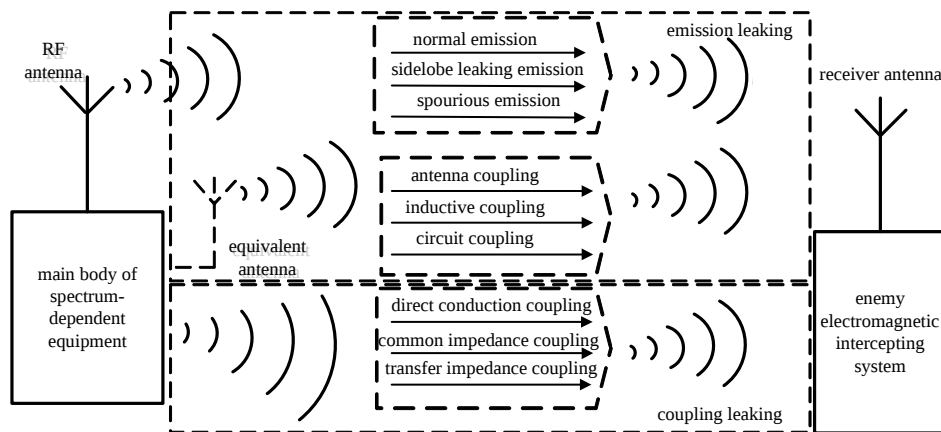


Fig.2 Way of the electromagnetic spectrum parameters leakage

图 2 电磁频谱参数泄露途径

传导泄露^[8]是指信息通过电源线、控制线、信号线、输入/输出接口线、地线向外传导造成的电磁频谱参数泄露,主要包括直接传导耦合、公共阻抗耦合和转移阻抗耦合等,敌方可通过其电磁窃收系统截获、提取和识别用频装备的地理位置信息、方位信息、使用规律等相关电磁频谱参数信息。

2.3 电磁频谱参数泄露原因

根据电磁频谱参数泄露途径可知,造成电磁频谱参数泄露的原因主要有:

1) 用频装备功率发射超标造成的电磁频谱参数泄露。用频装备操作者有可能为了克服干扰对用频装备战技术性能的影响,违规增加用频装备的发射功率,扩大了用频装备电磁信号的辐射范围,增大了用频装备向外辐射的电磁信号被第三方截获的概率,对电磁频谱参数安全造成了泄露。

2) 用频装备使用时机不对造成的电磁频谱参数泄露。由于情报信息不畅通,或者操作者不遵守相关命令要求而在敌方卫星过顶,侦察飞机、侦察船只以及地面侦察车和站等开展侦察活动时使用用频装备,从而导致用频装备的电磁频谱参数暴露在敌方的侦察系统面前,发生电磁频谱参数泄露。

3) 科研试验频率使用监管不严造成的电磁频谱参数泄露。在新研用频装备开展科研试验时,随意用频、违规用频等行为极易导致用频装备在科研试验阶段发生电磁频谱参数泄露。

4) 训练与作战频率区分不严格造成的电磁频谱参数泄露。在训练演习中,用频装备的训练频率可能受到对抗方的干扰难以使用,用频装备操作者违规改用作战频率,增加了敌方通过平时的侦收获取用频装备的作战频率的概率,给战时电磁频谱参数安全问题带来了隐患。

5) 用频装备部署不够合理造成的电磁频谱参数泄露。重大任务方案或作战预案制定者在制定用频装备部署方案时有可能因情报信息不够、技术手段不足、考虑因素不全等问题,将用频装备部署在敌方侦察力量的方向或范围内,从而导致电磁频谱参数被敌方窃取。

6) 安全意识不强、操作不规范造成的电磁频谱参数泄露。由于操作者对无形的电磁频谱重视不够,电磁频谱参数安全防范意识不强,加上其专业知识不够,用频装备的操作不够规范,有时过多追求用频装备性能的发挥,超标准辐射、违规使用等现象时有发生,电磁频谱参数在不知不觉中泄露出去。

3 电磁频谱参数泄露防护方法

电磁频谱参数泄露防护工作贯穿于整个重大任务的各个阶段,在此主要分别就任务筹划、任务实施和任务结束 3 个阶段中电磁频谱参数泄露防护来介绍电磁频谱参数泄露防护方法。

3.1 任务筹划阶段电磁频谱参数泄露防护

在任务筹划阶段,首先通过协调电磁频谱管理、电磁环境感知、电子对抗和装备保障等相关力量,成立电磁频谱参数泄露防护联管联控小组,明确联管联控小组职责,制定联管联控机制,收集相关信息,制定电磁频谱参数泄露防护预案,其具体流程如图3所示。

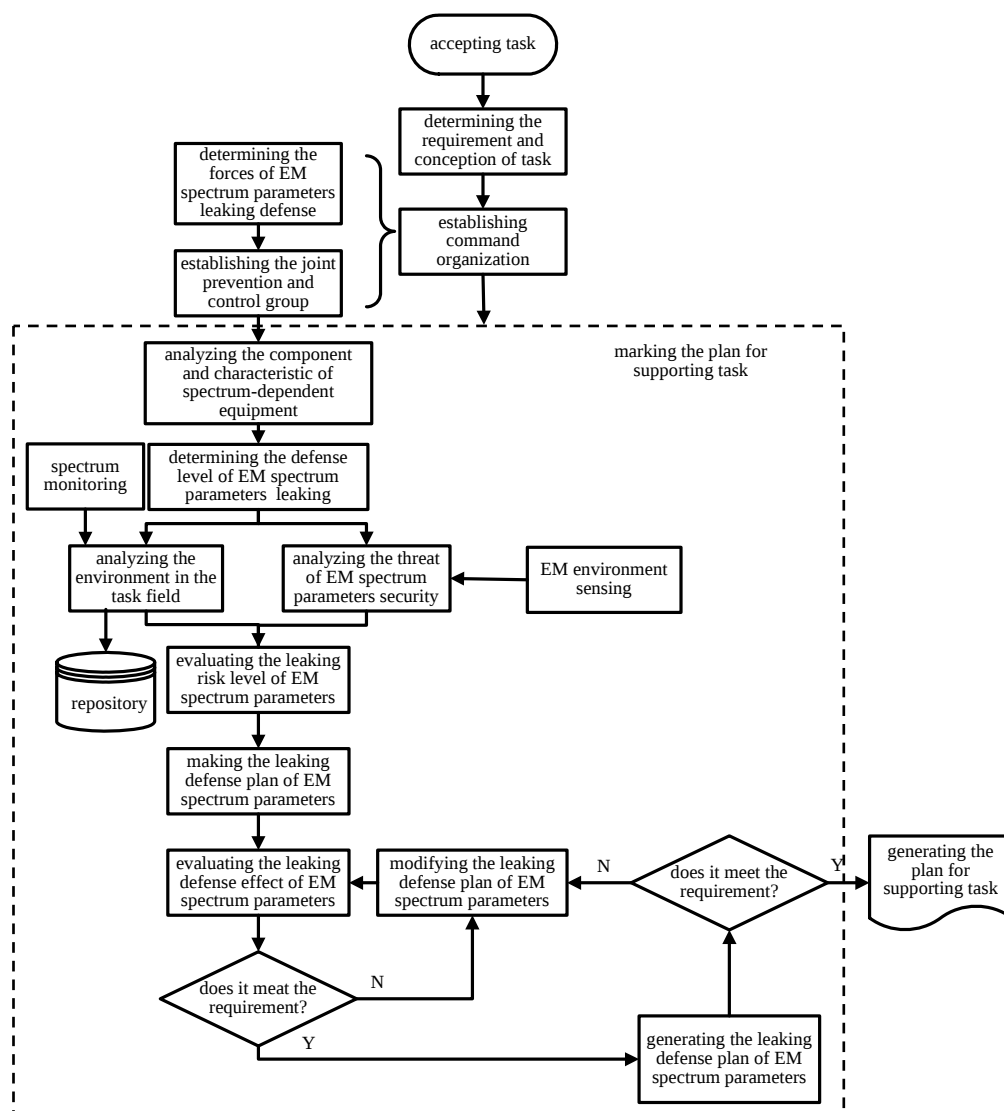


Fig.3 Defense process for electromagnetic spectrum parameters leakage in the stage of the task planning

图3 任务筹划阶段电磁频谱参数泄露防护流程

- 1) 熟悉用频装备编配情况,掌握用频装备的组织应用方案、频谱参数、收发特性、电磁环境效应等相关信息,明确电磁频谱参数泄露防护等级;
- 2) 掌握任务区域内可用电磁频谱资源,组织力量对任务区域内的自然背景噪声、背景电磁信号进行监测分析,掌握任务区域内的电磁环境数据,摸清任务区域内的地形地貌等地理信息、任务实施时间内的天气信息等影响电磁环境变化的其他因素;
- 3) 基于掌握的电磁环境数据和地理信息,根据任务实施方案和用频装备组织运用方案,适时开启相应的用频装备,利用电磁信号区域覆盖工具进行覆盖区域预测分析,预测各用频装备在任务区域或周边区域空间内的电磁信号强度分布情况,同时构建各个空间、各个时刻电磁环境模板,并存入到知识库中;
- 4) 基于电磁环境感知提供的情报信息和侦察信息,对敌方部署在演习作战区域附近的地面、海上、空中、天基的侦察力量、侦察装备性能和侦察规律进行分析;
- 5) 根据用频装备电磁频谱参数泄露防护等级要求和电磁频谱参数泄露风险等级划分,基于步骤3)和4)的分析结果,利用电磁频谱参数泄露风险评估工具对用频装备电磁频谱参数泄露风险进行评估;

6) 根据用频装备自身防护能力、开设地域特征和所配备的电子对抗装备能力, 起草电磁频谱参数泄露防护预案;

7) 利用电磁信号区域覆盖分析工具对采用防护措施后的用频装备正常工作时向外辐射的电磁信号覆盖区域进行预测分析, 利用电磁频谱参数泄露风险评估工具对其进行再次分析评估, 判断其是否满足用频装备电磁频谱参数泄露防护等级要求, 若满足, 则生成频率使用方案和电磁频谱参数泄露防护预案, 继续执行步骤 8), 若不满足, 则修改电磁频谱参数泄露防护预案, 并重复执行步骤 6);

8) 分析频率使用方案和电磁频谱参数泄露防护预案是否满足会影响任务执行过程中用频装备性能发挥要求, 如满足, 则将其纳入到任务实施方案中; 若不满足, 给出不满意的原因, 并对电磁频谱参数泄露防护预案进行修改, 并重复执行步骤 7) 和 8)。

3.2 任务实施阶段电磁频谱参数泄露防护

在任务开始实施后, 电磁频谱参数泄露防护联管联控小组将组织协调电磁频谱管理、电磁环境感知、电子对抗和用频装备使用等单位实施电磁频谱参数泄露防护, 确保电磁频谱参数泄露防护指挥顺畅, 信息交互畅通, 各分队间无缝协作, 其主要流程如图 4 所示。

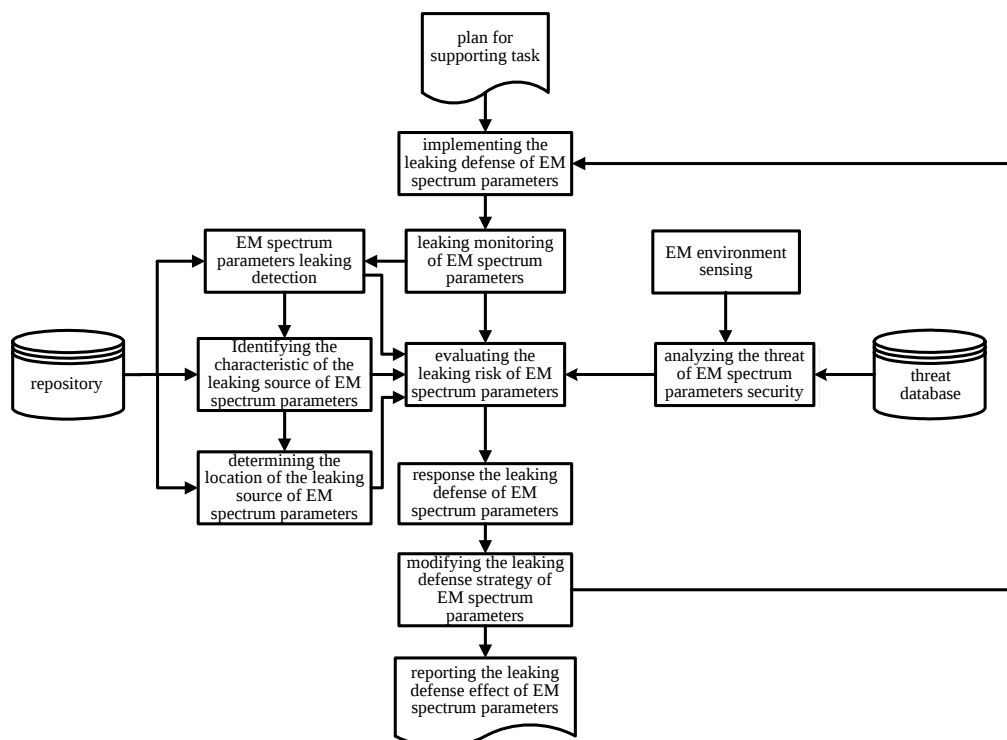


Fig.4 Defense process of electromagnetic spectrum parameters leakage in the stage of the task implementing

图 4 任务实施阶段电磁频谱参数泄露防护流程

1) 在任务开始后, 组织力量对任务区域及周边的电磁环境进行监测, 监测其用频装备电磁频谱参数泄露情况;

2) 组织技术人员对实时获取的监测数据进行分析处理, 基于任务筹划阶段构建的、且在任务推进过程中实时更新的知识库, 利用电磁频谱参数泄露检测工具, 判断是否存在电磁频谱参数泄露现象, 如存在, 则通过对辐射源的特征提取来识别其泄露源, 并综合利用电磁频谱泄露源测向定位设备和知识库提供的先验知识对泄露源进行测向定位;

3) 根据电磁环境感知实时提供的情报信息、侦察信息, 以及历史威胁数据, 分析敌对势力在任务区域及周边部署的侦察力量以及侦察装备性能, 摸清实施侦察活动的规律, 分析电磁频谱参数泄露面临的安全问题;

4) 根据电磁频谱参数泄露识别结果和电磁频谱参数泄露安全威胁, 利用电磁信号区域预测工具和电磁频谱参数风险评估工具, 综合考虑目前已采取的电磁频谱参数泄露防护措施, 评估用频装备电磁频谱参数泄露风险, 给出电磁频谱参数泄露风险等级;

5) 根据电磁频谱参数泄露风险评估结果,更新电磁频谱参数泄露防护预案,并及时向联管联控小组汇报,联管联控小组将针对电磁频谱参数泄露风险评估结果和预案修订情况,快速准确做出决策,对电磁频谱参数泄露问题做出及时响应,并将更新后电磁频谱参数泄露防护预案及时下发至各单位,以便其及时采取有效措施应对电磁频谱参数泄露。

3.3 任务结束阶段电磁频谱参数泄露防护

任务结束后电磁频谱参数泄露防护流程如图5所示。联管联控小组在演习作战任务结束后,将及时收集参与电磁频谱参数泄露防护工作的单位对电磁频谱参数泄露防护情况的反馈和意见,组织联管联控小组对此次电磁频谱参数泄露防护的组织、电磁频谱参数泄露防护环节、电磁频谱参数泄露防护措施等方面对电磁频谱参数泄露防护效果进行评估,查找电磁频谱参数泄露防护存在的问题,分析电磁频谱参数泄露防护措施应对各种威胁的有效性。同时从情报侦察信息有效性、及时性、电磁频谱参数泄露监测准确性、风险评估的可信性、主动防护的有效性、用频装备自身防护能力等方面对电磁频谱参数泄露防护进行评估,形成电磁频谱参数泄露防护工作建议,根据实际情况,修正电磁频谱参数泄露防护机制和规范,完善电磁频谱参数泄露防护工具手段,培养电磁频谱参数泄露防护人才队伍。

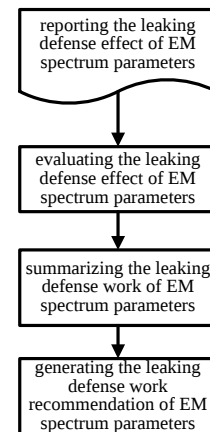


Fig.5 Defense process of electromagnetic spectrum parameters leakage in the stage of the task termination

图5 任务结束阶段电磁频谱参数泄露防护流程

4 结论

面对用频装备高密度大规模使用而引起的电磁频谱参数泄露给电磁频谱参数安全带来的巨大威胁和挑战,本文在分析电磁频谱参数泄露产生的危害的基础上,通过对电磁频谱参数泄露基本模式、途径及原因的分析研究,找到电磁频谱参数泄露机理,给出了电磁频谱参数防护方法流程,并经过试验验证了给出的方法流程的有效性,为开展电磁频谱参数泄露防护提供支撑。

参考文献:

- [1] 于江,段联国,杨健,等. 军地联合战场电磁频谱管理研究[J]. 现代电子技术, 2012(4):81-84. (YU Jian,DUAN Lianguo, YANG Jian,et al. Research on military-civilian-joint battlefield electromagnetic spectrum management[J]. Modern Electronics Technique, 2012(4):81-84.)
- [2] 王远昌,都诚,都世民. 信息系统的电磁泄漏及其防护初探[J]. 系统工程与电子技术, 2001,23(10):52-54,92. (WANG Yuanchang,DU Cheng,DU Shimin. Preliminary discussion on the electromagnetic leakage of information system and its protection[J]. Systems Engineering and Electronics, 2001,23(10):52-54,92.)
- [3] 程德胜,汪卫华,宣源. 信息技术设备的电磁泄漏及其防护研究[J]. 装备环境工程, 2008,5(1):95-98. (CHENG Desheng, WANG Weihua,XUAN Yuan. Study of the electromagnetic leakage and safeguard for the information technology equipment[J]. Equipment Environmental Engineering, 2008,5(1):95-98.)
- [4] 王利涛,郁滨. 信息技术设备电磁泄漏建模与防护[J]. 计算机工程与设计, 2013,34(1):49-54. (WANG Litao,YU Bin. Modeling and security protection on electromagnetic compromising emanations of information technology equipment[J]. Computer Engineering and Design, 2013,34(1):49-54.)
- [5] 张余,柳永祥,陈勇,等. 用频装备电磁频谱参数防泄露问题研究[D]. 天津:兵器工业出版社,2015. (ZHANG Yu,LIU Yongxiang,CHEN Yong,et al. Research on the defense of electromagnetic spectrum parameters leaking for spectrum-dependent equipment[D]. Tianjin,China:Ordnance Industry Publishing House, 2015.)
- [6] 吴昊,柳永祥,赵杭生. 用频装备电磁频谱参数安全风险若干问题探讨[J]. 现代军事通信, 2012,20(1):54-58. (WU Hao,LIU Yongxiang,ZHAO Hangsheng. Research on some problems of the electromagnetic spectrum parameters security for spectrum-dependent equipment[J]. Journal of Modern Military Communications, 2012,20(1):54-58.)
- [7] 徐平,万海军,张勇,等. 舰船信息技术设备电磁泄露研究[J]. 微波学报, 2012(8):390-392. (XU Ping,WAN Haijun, ZHANG Yong,et al. Research on electromagnetic information leakage in information technology equipment of naval ship[J]. Journal of Microwaves, 2012(8):390-392.)

(下转第 1079 页)